



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,103	06/30/2000	Christopher L. Hamlin	K35A0631	1085

26332 7590 05/13/2004

WESTERN DIGITAL CORP.
20511 LAKE FOREST DRIVE
C205 - INTELLECTUAL PROPERTY DEPARTMENT
LAKE FOREST, CA 92630

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 05/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

25

Office Action Summary	Application No. 09/608,103	Applicant(s) HAMLIN, CHRISTOPHER L.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 4/26/2004, the following **claims 1-16** are presented for examination.
2. The amendments to the specification, pages 2-3, filed on 4/26/2004 have been considered. The objection to the drawing has been withdrawn.
3. Applicant's arguments, pages 4-8, filed on 4/26/2004, with respect to the rejection of claims 1-16 under 35 USC 103 (a) have been fully considered but are not persuasive. Regarding claim 1, Applicant argues (pages 3-5) that the reference does not teach the limitation of wherein the encrypted message comprises ciphertext data and client drive ID identifying the client disk drive. Applicant is arguing the difference between the prior art encrypted message and the encrypted message in claim 1. Claims directed to an apparatus must be distinguished from the prior art in terms of the structure rather than function. See MPEP § 2114. Applicant also argues on pages 6 and 7 about a function (what the key is comprised of) rather than the structure of (key generator) disclosed in the prior art (see MPEP § 2114). Applicant did not overcome the rejection. Examiner respectfully asserts that the prior art references teach the structural limitations claimed by Applicant's apparatus.

Examiner retains the same rejection of claims 1-16 under 35 USC 103(a).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4.1 **Claims 1-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,397,333 to **Sohne et al.** in view of US Pub. US 2001/0032088 to **Utsumi et al.** and in view of US Patent 5,805,699 to **Akiyama et al.**

4.2 **As per claims 1 and 9, Sohne et al.** substantially teaches a secure disk drive comprising: a memory for storing data (see column 4, line 64); (b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a device ID (see column 3, lines 8-11); (c) a secure drive key (see column 3, lines 39-41); (d) an internal drive ID (see column 6, line 25); (f) an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and the client drive key (see column 3, lines 60-64); (g) a data processor comprising: a message input for receiving the encrypted message from the client disk drive; a data output for

outputting the ciphertext data to be written to the disk (see column 4, lines 60-64); a data input for receiving ciphertext data read from the disk (see drawings); an enable input for receiving the enable signal for enabling the data processor (see column 4, lines 44-47 and lines 64-67); a key input for receiving the internal drive key (see drawings). **Sohne et al.** does not explicitly teach storing data on a disk. It is well known in the art that a disk drive comprising disk to store data. **Sohne et al.** does not explicitly teach using the ID of the originator. However, **Utsumi et al.** in an analogous art teaches (b) an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive (see page 1, paragraph 007). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the secure disk drive of **Sohne et al.** to use the first media ID identifying the first media as taught by **Utsumi et al.** to identify one's own self (see page 1, paragraph 007). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Utsumi et al.** so as to identify one's own self.

Sohne et al. substantially teaches a key generator for generating a dynamic key. **Sohne et al.** does not explicitly teach generating a client drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key. However, **Akiyama et al.** in an analogous art teaches (e) a key generator for generating a client drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key; (see column 7, lines 49-53). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the secure disk drive of **Sohne et al.** to use a key generator for generating a client

drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key as taught by **Akiyama et al.** to encrypt and manage the keys at the software license center (see column 7, lines 49-53). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Akiyama et al.** so as encrypt and to manage the keys.

Sohne et al. further teaches outputting the data set comprising the internal drive ID (see column 3, lines 30-38 see also column 4, line 60 through column 5, line 4). However, **Sohne et al.** does not explicitly teach outputting a reply comprising a message authentication code the cipher text data and the internal drive ID. A reply comprising a message authentication code generated by a secret key is well known in the art and admitted by Applicant in the prior art. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the secure disk drive of **Sohne et al.** to outputting a reply comprising a message authentication code cipher text data read from the disk and the internal drive ID for authentication purpose. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Akiyama et al.** for authentication purpose.

As per claims 2 and 10, Sohne et al. discloses the limitation of using a secure drive key that is immutable (see column 3, lines 37-38).

As per claims 3 and 11, Sohne et al. discloses the limitation of using a secure drive key that is mutable (see column 3, lines 19-23).

As per claims 4 and 12, **Sohne et al.** discloses the limitation of wherein the access rights of the client drive ID are verified by the content provider and the authenticator comprises a means for verifying the data set against its serial number and the public key. **Sohne et al.** does not explicitly teach wherein the authenticator comprises a means for verifying the access rights of the client drive ID. However, **Akiyama et al.** in an analogous art teaches an apparatus for devolving the right to use contents from a first storage medium to a second storage medium based client drive ID identifying the client disk drive (see page 1, paragraphs 002, 007, and 0013). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the secure disk drive of **Sohne et al.** to use authenticator comprises a means for verifying the access rights of the client drive ID as taught by **Akiyama et al.** to prevent unfair use of a person who is not entitled to the right of using (see pages 2-3, paragraph 0013). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Akiyama et al.** so as to prevent unfair use of a person who is not entitled to the right of using.

As per claims 5-7 and 13-15, the limitation of wherein the secure drive key, key generator and authenticator comprising tamper resistant circuitry are well known in the art.

As per claims 8 and 16, **Sohne et al.** discloses the limitation of wherein the data processor further comprises cryptographic facilities (see column 4, lines 35-67).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

ce

Carl Colin
Patent Examiner
May 3, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100